Unleashing the power of innovative aerospace technology....

@olumns

Air Force Research Laboratory
AFRL

news@*afrl*

Summer 1999 **Official voice of the Air Force Research Laboratory**

CIO Topics

Viruses and hoaxes; be on the lookout

Office culture these days lends itself to camaraderie and close quarters. This gives many of us such a sense of security that it is easy to forget that Internet terrorism goes on. Sometimes simply running a program that is attached to an e-mail message could initiate a virus that wreaks havoc on a computer's internal functions and may render office hardware useless. It is important to be familiar with the types of problems that are associated with these viruses and any warning signs that could prevent computer systems from becoming infected.

We have seen terrorism in recent months with the Melissa virus, among others. The Melissa virus affected machines with certain Word 97 or Word 2000 programs. Melissa was sent as an e-mail with the subject line, "Important Message From [name]." When the Word attachment that accompanied the e-mail was opened, the virus lowered the macro security settings to permit all macros to run when future documents were opened. Therefore, the user would not be notified when the virus was automatically executed on the hard drive.

In some cases, the virus propagated itself by sending the same initial message to the first 50 people on an infected computer's address book. If one of the first 50 was a mailing list, everyone on the list would get the message. This virus specifically targeted computers that used Microsoft Outlook. In other cases, it modified and damaged Word documents already saved to a piece of hardware.

In a short time, Melissa was able to tie up mail servers and significantly damage computer systems around the country.

Aside from the obvious problems these viruses have created, a lesser-known problem also accompanies this phenomenon – virus hoaxes. Sooner or later you may get an e-mail warning you not to open an e-mail with the subject line "Good Times," "AOL4Free" or "Penpal Greetings" because they contain a virus.

These e-mail warnings tell you that an e-mail (without any attachments) a user received is specially encoded with a virus that will destroy hardware from the inside out.

The fact is, you cannot get a virus by merely opening an e-mail message. An e-mail message is just plain text and contains no code. This means that it cannot do anything detrimental to a user's system.

The practice that makes these hoaxes damaging to the internal functions of government and business offices is the last line of the e-mail message that tells the reader to "send the message to all of your friends." The fear generated by these hoax e-mail messages results in mass chain mail. The Melissa virus automatically generates 50 e-mail messages to people stored on a computer address book. A user is doing the same amount of damage *willingly* if he or she forwards these hoax e-mails to several friends.

If you ever receive an e-mail like this, there is a net index of Computer Incident Advisory Capability at the U.S. Department of Energy that will help you determine its validity. This index is located at http://ciac.llnl.gov/ciac/CIACHoaxes.html.

Another common myth is that the JPEG or GIF pictures attached to an e-mail can contain viruses. This is not true.

The files that can contain viruses are attached to an e-mail (i.e. programs, Word documents, etc.), not pictures. But even these viruses cannot infect your computer when you simply download or open mail. The only way for them to infect your computer is if you purposely run the attached program or open an infected Word document.

Knowing this, there are a few steps one can take to eliminate the problems associated with viruses. First, pay attention to all e-mails that have attachments. If a sender is not someone familiar to you it may be wise to report this to the Corporate Information Office rather than to open it and risk activating a virus. If you know the sender, but were not expecting anything from him or her or if the e-mail was sent at an unusual time (i.e. 2 a.m.), be wary of it.

Similarly, if you receive a virus hoax, contact your computer system security officer *before* passing the virus

warning on to anyone else. These hoaxes operate like a chain letter and merely waste time and create an unnecessary panic. The information will be forwarded to the Air Force Computer Emergency Response Team , or AFCERT, for verification. If the information turns out to be accurate, the team will work with the major anti-virus companies to ensure a fix or "fix patch" is produced to counteract the virus. Because of proactive response by Air Force Materiel Command Headquarters and all Air Force Research Laboratory system administrators, the effective downtime of Melissa was measured in hours instead of days, unlike the problems experienced by some major corporations.

A little bit of caution can save you and your colleagues an immense amount of time and energy. **@**